Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF TRANSACTION NETWORK SERVICES, INC.

Transaction Network Services, Inc. ("TNS"), by its attorneys, hereby provides comments in response to the Further Notices of Proposed Rulemaking ("FNPRM") issued by the Federal Communications Commission ("FCC" or "Commission") in the above-referenced dockets.[1] In the FNPRM, the FCC seeks comment on, among other issues, whether to require gateway providers to block calls that are highly likely to be illegal based on reasonable analytics, and if so, whether gateway providers should receive a safe harbor for this blocking.[2] The Commission also asks whether it should further define what constitutes "reasonable analytics."[3] TNS does not take a position on whether or not the Commission should mandate call blocking by gateway providers, but if it does require blocking, it should grant these providers and their third party vendors a safe harbor from liability for erroneous blocking or non-blocking of calls. The FCC also should continue to refrain from further specifying what constitutes "reasonable analytics" in

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59 and WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105 (rel. Oct. 1, 2021) ("FNPRM").

[2] *Id.* at ¶¶ 66, 77.

[3] *Id.* at ¶ 70.

order to give providers flexibility to determine what methodology best enables them to identify highly likely unlawful calls.

As one of the leading analytics engines ("AE") supplying robocall mitigation tools to carriers and subscribers, TNS continues to support the Commission's multi-faceted effort to combat illegal robocalls. TNS' Call Guardian service is a robocall detection solution implemented by four of the six largest wireless carriers in the United States, by major cable VoIP providers and over a hundred rural wireline and wireless carriers. Call Guardian utilizes information from over 1 billion signaling transactions per day traversing the TNS signaling network to differentiate legitimate users of communications services from illegal and unwanted calls. Call Guardian integrates this data with numerous other industry data sources, including historical reputation information, STIR/SHAKEN parameters, and crowd-sourced data, to analyze calls in real-time. It uses this analysis to determine a Telephone Number Reputation score and category that its voice service provider partners use to make decisions on how to handle calls traversing their networks. Call Guardian's dynamic scoring system constantly re-assess calls to spot suspicious behavior and to keep pace with evolving tactics used by bad actors seeking to perpetrate scams and other malicious behavior. Call Guardian has proven effective in identifying suspect calls and allowing providers to mitigate unlawful and unwanted robocalls.

Safe Harbor. Gateway providers should receive the same safe harbor that terminating providers receive. The Commission's current rules permit terminating voice service providers to engage in network-based blocking without any opt-out requirement for calls that are highly likely to be unlawful based on reasonable analytics, so long as the blocking complies with certain requirements.[4] If the Commission mandates that gateway providers block calls that are highly likely to be unlawful based on reasonable analytics, it should extend the safe harbor to these providers, so long as the blocking is in good faith and similarly requires the providers to incorporate caller ID authentication information where available and apply all analytics in a non-discriminatory, competitively neutral manner, as the Commission proposes.[5]

Providing gateway providers with a safe harbor from liability protection is crucial to encourage them to adopt zealous call analytics to identify and block calls that are highly likely to be unlawful based on reasonable analytics. The FNPRM notes that "previous safe harbors were designed to incent blocking by ensuring that providers do not face liability for good faith blocking."[6] Since the Commission proposes to make blocking by gateway providers mandatory, it asks whether it is necessary to give them a safe harbor[7]—it is. The FNPRM acknowledges that even with a requirement to block highly likely unlawful calls based on reasonable analytics, the

[4] Specifically, terminating providers must: 1) incorporate caller ID authentication information designed to identify calls and call patterns that are highly likely to be illegal; 2) manage the blocking with human oversight and network monitoring sufficient to ensure that it blocks only calls that are highly likely to be illegal, which must include a process that reasonably determines that the particular call pattern is highly likely to be illegal prior to blocking calls that are part of that pattern; (3) cease blocking calls that are part of the call pattern as soon as the provider has actual knowledge that the blocked calls are likely lawful; (4) apply all analytics in a non-discriminatory, competitively neutral manner; (5) disclose to consumers that it is engaging in such blocking; (6) provide blocking services with no additional line-item charge to consumers; and (7) provide, without a line item charge to the caller, certain redress set forth in the rules. *See* 47 CFR § 64.1200(k)(11).

[5] FNPRM at ¶ 66. Similarly, if blocking is made voluntary, a safe harbor is appropriate to encourage more providers to deploy the blocking tools.

[6] *Id.* at ¶ 77.

[7] *Id.*

call blocking can be over- or under-inclusive.[8] Without a safe harbor, gateway providers are at risk of liability under both outcomes.

On the one hand, a provider that makes use of comparatively conservative blocking analytics may be subject to liability by under-blocking. For example, a call recipient may assert that the provider has failed to meet the FCC's requirement to block calls that are highly likely to be unlawful. Such a provider may also be subject to blocking from downstream providers, and particularly terminating providers who do have a safe harbor for blocking those calls. Even if such claims do not arise in every instance, the disincentive for gateway providers to be aggressive contradicts the FCC's goal in this proceeding to maximize the number of unlawful calls that are blocked, resulting in ongoing harm to consumers.

On the other hand, a provider that uses comparatively aggressive blocking analytics may be subject to liability by over-blocking. While TNS sees very little evidence of "false positives" (*i.e.*, calls rated negatively that should be scored positively), the most effective blocking of calls, which the Commission seemingly desires, may result in some instances of legitimate calls being blocked. In that case, the FCC could choose to conclude that the blocking was beyond reasonable, even when it is otherwise consistent with the Commission's mandate. The gateway providers would also risk liability from call originators and end users for erroneous blocking of calls. This might be the case even when call originators are provided with avenues to address when they believe their calls are being erroneously blocked.[9]

[8] *Id.* at ¶ 67. This over- and under-inclusiveness cannot be resolved by further defining reasonable analytics because analytics are necessarily dynamic, as explained below.

[9] For example, TNS provides a free mechanism for call originators and enterprises to provide feedback into its reputation scoring. They can use this mechanism to identify potential inaccuracies in analytics data and to engage with TNS on how their numbers are scored. This portal is easily accessed at www.reportarobocall.com.

The Commission should not place gateway providers in this dilemma. Instead, it should extend the call blocking safe harbor to incentivize gateway providers to fine-tune their call analytics so that they are maximizing blocking of highly likely unlawful calls and minimize erroneous call blocking.

As TNS has discussed in related contexts, the benefits of such a safe harbor could be undermined if the safe harbor does not extend to the voice service providers' vendors as well.[10] If a safe harbor protected the voice service provider, but allowed a disgruntled call originator or end user to pursue claims against the underlying AE or against a vendor that provided a call blocking solution to the service provider, the benefit of a safe harbor could be lost. Under these circumstances, vendors may be reluctant to provide innovative solutions to identify calls that are highly likely to be unlawful within the scope of the Commission's parameters, simply because they could face liability if they were to do so (even if the voice service provider were protected from such liability). Therefore, the Commission should include gateway provider vendors or agents within the safe harbor for blocking.

Meaning of "Reasonable Analytics." To ensure that AE providers can continue to innovate their services and prevent bad actors from circumventing these tools, the Commission should decline to provide further guidance on what constitutes "reasonable analytics" for identifying highly likely unlawful calls. Determining whether calls are highly likely to be unlawful depends on a multitude of factors, many of which the Commission identified in its 2019 Call Blocking Declaratory Ruling.[11] TNS' Call Guardian utilizes these and other factors, in

[10] *See* Comments of Transaction Network Services, Inc., CG Docket No. 20-93, 4 (June 19, 2020).

[11] A reasonable call analytics based program may block calls "based on a combination of factors, such as: large bursts of calls in a short timeframe; low average call duration; low call completion ratios; invalid numbers placing a large volume of calls; common Caller

combination with real-time user feedback and other information from its provider partners, such as user complaints and international toll charges, as part of a dynamic and holistic analysis of calls to properly score them. Much of this information is necessarily fluid and will change frequently as the calling patterns of illegal robocallers change, often from minute to minute rather than over days or weeks. The algorithm feeding the Call Guardian analysis is constantly reviewed and updated through machine learning, taking into account new sources of data and the new tactics used by illegal callers to avoid detection. As the Commission has rightly observed in the past, "rigid blocking rules" can be counter-productive and "could impede the ability of voice service providers to develop dynamic blocking schemes that evolve with calling patterns,"[12] like those used by TNS' Call Guardian. Particularly in the context of identifying calls that are highly likely to be unlawful, the Commission should continue to allow providers and their vendors discretion in determining the appropriate methodology and processes for identifying harmful calls to keep up with the changing nature of the threats.

* * *

For the foregoing reasons, if the Commission mandates that gateway providers block calls that are highly likely to be unlawful based on reasonable analytics, it should give those providers and their vendors a safe harbor for their good faith call blocking efforts and continue to

ID Name (CNAM) values across voice service providers; a large volume of complaints related to a suspect line; sequential dialing patterns; neighbor spoofing patterns; patterns that indicate TCPA or other contract violations; correlation of network data with data from regulators, consumers, and other carriers; and comparison of dialed numbers to the National Do Not Call Registry." *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59 and WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51, ¶ 35 (rel. June 7, 2019).

[12] *Id.* at ¶ 35.

allow providers and vendors flexibility in determining the best methodology for blocking such calls.

Respectfully Submitted,

TRANSACTION NETWORK SERVICES, INC.

Steven A. Augustino
Chris M. Laughlin
KELLEY DRYE & WARREN, LLP
3050 K Street NW
Suite 400
Washington, DC 20007
(202) 342-8400
saugustino@kelleydrye.com

Counsel to Transaction Network Services, Inc.

James Tyrrell
Paul Florack
TRANSACTION NETWORK SERVICES, INC.
10740 Parkridge Blvd.
Suite 100
Reston, VA 20191
(703) 453-8300
jtyrrell@tnsi.com
pflorack@tnsi.com

December 10, 2021